

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-018168
 (43)Date of publication of application : 17.01.2003

(51)Int.CI. H04L 12/28
 H04L 9/14

(21)Application number : 2002-105879 (71)Applicant : LG ELECTRONICS INC
 (22)Date of filing : 08.04.2002 (72)Inventor : YI SEUNG JUNE

(30)Priority

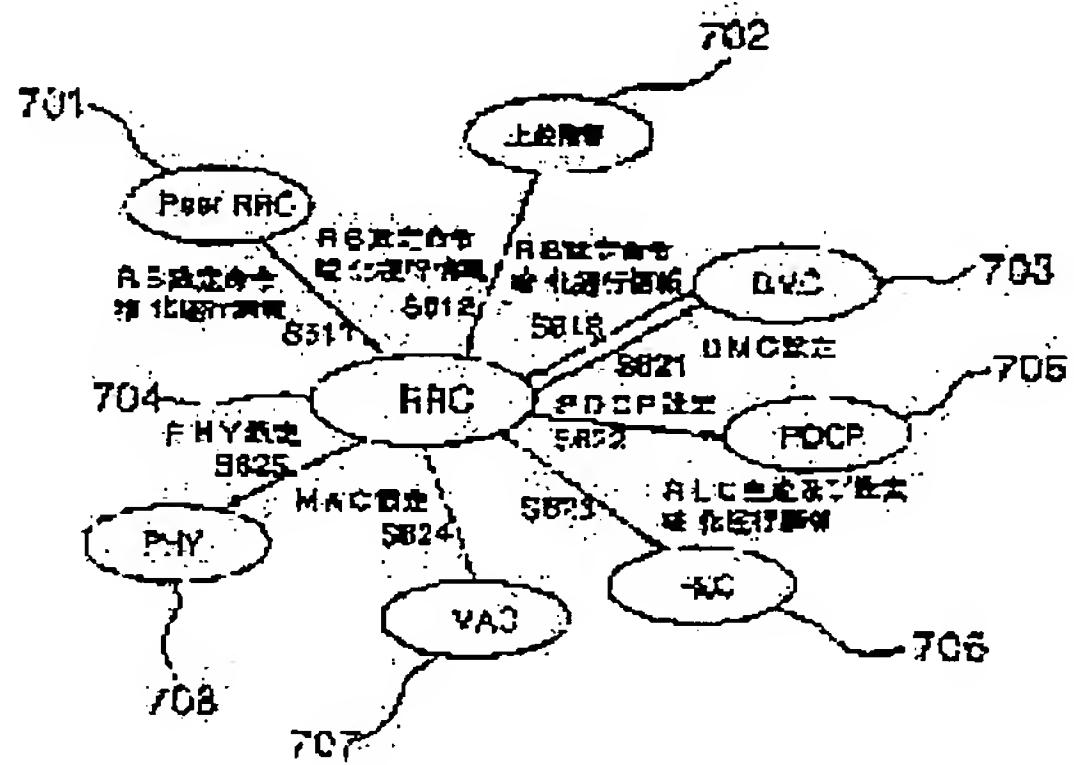
Priority number : 2001 200118519 Priority date : 07.04.2001 Priority country : KR

(54) RADIO-BEARER SETTING METHOD FOR MOBILE COMMUNICATION SYSTEM, CIPHERING EXECUTING METHOD, CIPHERING ALTERING METHOD FOR RADIO BEARER, AND DATA-CIPHERING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method where by setting also in a setting time whether or not each radio bearer can be ciphered, the cipherings of respective radio bearers are selectively conducted by each radio bearer.

SOLUTION: In the radio-bearer setting method of a radio interface protocol, there are included a step for transferring ciphering executing informations from predetermined hierarchies to a radio-resource control(RRC) hierarchy (704); a step for transferring the ciphering executing informations from the radio-resource control hierarchy (704) to a radio-link control(RLC) hierarchy (706); and a step for ciphering data by ciphering executing informations in the radio-link control hierarchy (706).



LEGAL STATUS

[Date of request for examination] 08.04.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2003-18168

(P2003-18168A)

(43)公開日 平成15年1月17日(2003.1.17)

(51)Int.Cl.⁷

H 04 L 12/28
9/14

識別記号

3 0 0

F I

H 04 L 12/28
9/00

テマコード(参考)

3 0 0 Z 5 J 1 0 4
6 4 1 5 K 0 3 3

審査請求 未請求 請求項の数21 OL (全 14 頁)

(21)出願番号 特願2002-105879(P2002-105879)
(22)出願日 平成14年4月8日(2002.4.8)
(31)優先権主張番号 2001-018519
(32)優先日 平成13年4月7日(2001.4.7)
(33)優先権主張国 韓国(KR)

(71)出願人 590001669
エルジー電子株式会社
大韓民国、ソウル特別市永登浦区汝矣島洞
20
(72)発明者 スン ジョン イ
大韓民国 ソウル、カンナムーク、ケ
ボードン、テュン アパートメント
303-403
(74)代理人 100078282
弁理士 山本 秀策

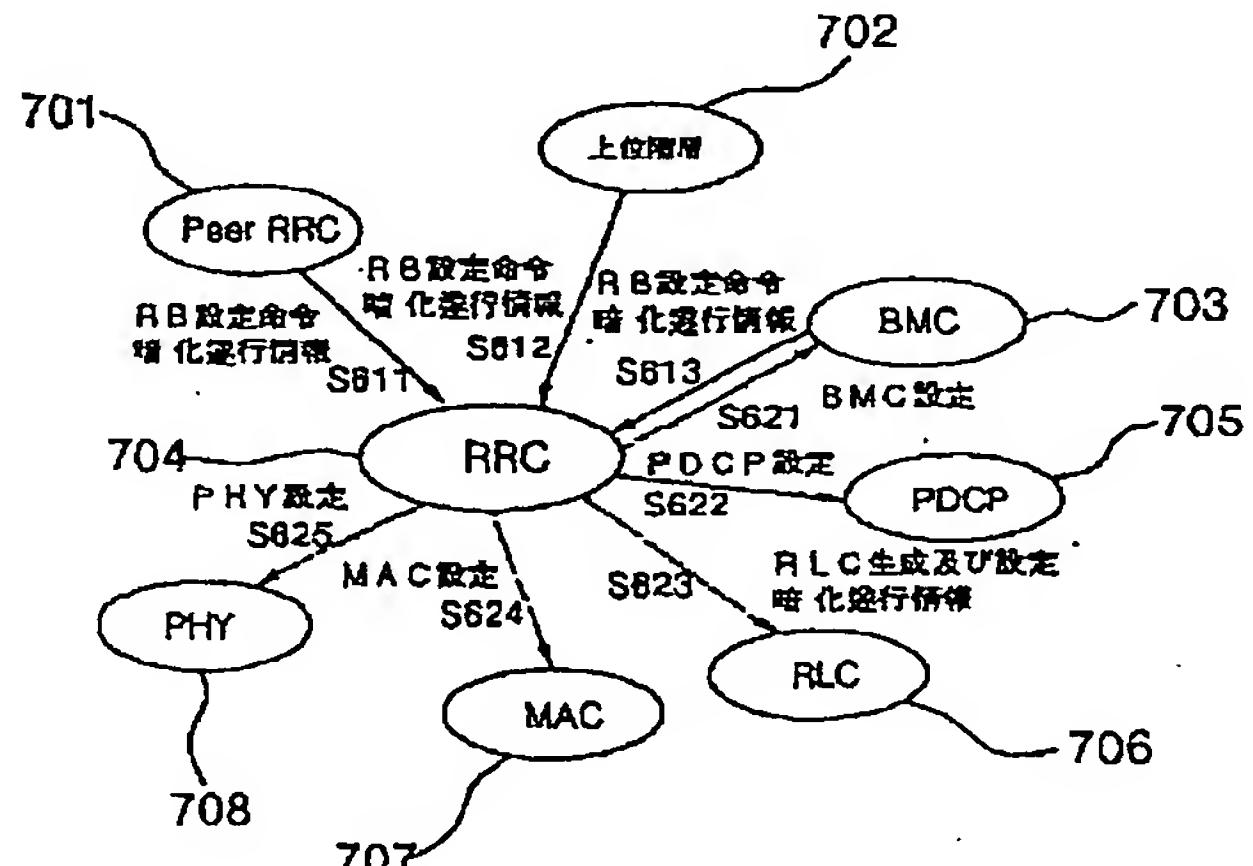
最終頁に続く

(54)【発明の名称】 移動通信システムの無線ペアラー設定方法、暗号化遂行方法、無線ペアラーの暗号化変更方法およびデータ暗号化方法

(57)【要約】

【課題】本発明は、無線ペアラー設定時にその暗号化の可否も共に設定して、各無線ペアラー別に暗号化を選択して行うための方法を提供する。

【解決手段】本発明は、無線インターフェースプロトコルの無線ペアラーを設定する方法において、所定階層から無線資源制御(RRC)階層704に暗号化遂行情報を伝達する段階と、無線資源制御階層704から暗号化遂行情報を無線リンク制御(RLC)階層706に伝達する段階と、無線リンク制御階層706で暗号化遂行情報によってデータを暗号化させる段階とを含む。



【特許請求の範囲】

【請求項1】 無線インターフェースプロトコルの無線ベアラーを設定する方法において、所定階層から無線資源制御(RRC)階層に暗号化遂行情報を伝達する段階；前記無線資源制御階層で前記暗号化遂行情報を無線リンク制御(RLC)階層に伝達する段階；及び、前記無線リンク制御階層で前記暗号化遂行情報によってデータを暗号化させる段階を含んでなることを特徴とする無線ベアラー設定方法。

【請求項2】 前記所定階層から前記無線資源制御(RRC)階層に無線ベアラー設定情報を伝達する段階；及び、前記無線資源制御階層で前記無線ベアラー設定情報によって下位階層の無線ベアラーを設定する段階をさらに含むことを特徴とする請求項1に記載の無線ベアラー設定方法。

【請求項3】 前記所定階層は上位階層、ブロードキャスト/マルチキャスト制御(BMC)階層及びピア無線資源制御(peer RRC)階層を含むことを特徴とする請求項1に記載の無線ベアラー設定方法。

【請求項4】 前記暗号化遂行情報はNASメッセージを利用して前記上位階層から伝達されることを特徴とする請求項1に記載の無線ベアラー設定方法。

【請求項5】 前記無線リンク制御(RLC)階層は無線ベアラー設定時に生成されることを特徴とする請求項1に記載の無線ベアラー設定方法。

【請求項6】 設定された無線ベアラーを利用してデータサービスの提供途中に前記暗号化遂行情報が変更できることを特徴とする請求項1に記載の無線ベアラー設定方法。

【請求項7】 前記暗号化遂行情報の変更は前記所定階層から伝達される暗号識別子の変更によって行われることを特徴とする請求項6に記載の無線ベアラー設定方法。

【請求項8】 無線インターフェースプロトコルの暗号化を行う方法において、無線ベアラー設定要求によって所定階層から無線資源制御(RRC)階層に暗号化遂行情報及び無線ベアラー設定情報を伝達する段階；前記無線資源制御階層で前記無線ベアラー設定情報によって下位階層の無線ベアラーを設定する段階；前記無線ベアラー設定要求に応答して無線リンク制御(RLC)階層を生成する段階；及び、前記無線リンク制御階層で前記暗号化遂行情報によってデータを暗号化させる段階を含んでなることを特徴とする暗号化遂行方法。

【請求項9】 前記無線ベアラー設定要求の発生時ごとに新しく生成される無線リンク制御階層により暗号化が行われることを特徴とする請求項8に記載の暗号化遂行方法。

【請求項10】 前記所定階層は上位階層、ブロードキャスト/マルチキャスト制御(BMC)階層及びピア無線資源制御(peer RRC)階層を含むことを特徴とする請求項8に記載の暗号化遂行方法。

【請求項11】 前記暗号化遂行情報は暗号識別子であることを特徴とする請求項8に記載の暗号化遂行方法。

【請求項12】 暗号化を変更する方法において、無線リンク制御(RLC)階層で所定階層から伝達された暗号化遂行情報によってデータの暗号化を行う段階；前記所定階層で前記暗号化遂行情報を更新する段階；前記更新の暗号化遂行情報を前記無線リンク制御階層に伝達する段階；及び、

前記更新の暗号化遂行情報によって前記データの暗号化を行う段階を含んでなることを特徴とする無線ベアラーの暗号化変更方法。

【請求項13】 前記所定階層は上位階層、ブロードキャスト/マルチキャスト制御(BMC)階層及びピア無線資源制御(peer RRC)階層を含むことを特徴とする請求項12に記載の無線ベアラーの暗号化変更方法。

【請求項14】 前記暗号化遂行情報は暗号化の可否を示すことを特徴とする請求項12に記載の無線ベアラーの暗号化変更方法。

【請求項15】 前記暗号化遂行情報は暗号識別子であることを特徴とする請求項12に記載の無線ベアラーの暗号化変更方法。

【請求項16】 移動通信送受信装置において、無線資源制御(RRC)階層がデータサービス要求に対応する無線リンク制御(RLC)階層と無線ベアラーを設定する段階；前記無線資源制御階層で前記無線ベアラーに対する暗号化遂行情報を前記無線リンク制御階層に伝達する段階；及び、

前記無線リンク制御階層で前記暗号化遂行情報によって前記無線ベアラーを通じて伝達されるデータを暗号化する段階を含んでなることを特徴とするデータ暗号化方法。

【請求項17】 前記無線資源制御階層が所定階層からデータサービス要求とこれに対する暗号化遂行情報を伝達される段階をさらに含むことを特徴とする請求項16に記載のデータ暗号化方法。

【請求項18】 前記無線資源制御階層が前記所定階層から無線ベアラー設定情報を伝達されることを特徴とする請求項17に記載のデータ暗号化方法。

【請求項19】 前記所定階層は上位階層、ブロードキャスト/マルチキャスト制御階層、ピア無線資源制御階層の何れか一つであることを特徴とする請求項17に記載のデータ暗号化方法。

【請求項20】 前記設定された無線ベアラーを利用してデータサービスの提供途中に前記暗号化遂行情報が変更できることを特徴とする請求項16に記載のデータ暗号化方法。

【請求項21】前記暗号化遂行情報の変更は前記所定階層から伝達される暗号識別子の変更によって行われることを特徴とする請求項20に記載のデータ暗号化方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は移動通信システムに関し、無線資源制御(RRC)階層が無線ベアラーの設定時にその暗号化の可否も共に設定し、合わせて、設定された暗号化の可否を無線ベアラー別に変更できる方法に関する。

【0002】

【従来の技術】第3世代ネットワーク及び無線接続方式である3GPP(3rd Generation Partnership Project)における無線資源制御(RRC:Radio Resource Control)階層は各階層を制御するプロトコル階層である。前記RRC階層は、開放型システム間相互接続(OSI:Open Systems Interconnection)基準モデルの下位3個階層中の第3階層に該当する。前記各階層はパケットデータ収斂プロトコル(PDCP:Packet Data Convergence Protocol)階層、ブロードキャスト/マルチキャスト(BMC:Broadcast/Multicast Control)階層、無線リンク制御(RLC:Radio Link Control)階層、媒体接続制御(MAC:Medium Access Control)階層及び物理(Physical)階層を含む。ここで、物理階層は第1階層に含まれ、残り階層すなわちPDCP階層、BMC階層、RLC階層及びMAC階層は第2階層に含まれる。

【0003】図1は、3GPPの無線インターフェースプロトコルの構造を示す構成図である。

【0004】図1を参照すれば、前記無線インターフェースプロトコルは、各階層を制御するRRC階層10、パケットデータの転送に使用されるPDCP階層21、ブロードキャスト及びマルチキャストデータの転送に使用されるBMC階層22、データリンク階層としてフレーム制御を担当するRLC階層23、前記RLC階層23からデータを受けて論理チャンネルと転送チャンネル(T-transport Channel)との間の適切な対応(Mapping)関係を利用してデータを伝達するMAC階層24、及び実際物理チャンネルにデータを載せて無線区間に転送するPHY階層30を含んでなる。

【0005】前記RRC階層10は、制御平面だけで定義され、RB等の設定、再設定及び解除と関連して転送チャンネル及び物理チャンネル間の制御を担当する。このとき、前記RBの設定は特定サービスを提供するために必要なプロトコル階層及びチャンネルの特性を規定し、それぞれの具体的なパラメーター及び動作方法を設定する過程を意味する。

【0006】前記PDCP階層21は、RLC階層の上位に位置し、IPv4またはIPv6のようなネットワークプロトコルを通じて転送されるデータ等が無線イン

ターフェースを通じて転送されるのに適合するようにする。

【0007】前記BMC階層22は、CBC(Cell Broadcast Center)から伝達されたメッセージを無線インターフェースを通じて転送されるようにする。換言すれば、前記BMC階層22は端末に転送されるセル発送メッセージ(Cell Broadcast Message)をスケジューリングして転送するもので、一般的に無応答モード(UM:Unacknowledged Mode)で動作するRLC階層23を通じてデータを転送する。

【0008】前記RLC階層23は、上位階層から転送されたRLC SDUの分割及び連結(Segmentation and Concatenation)機能のために転送に適合しているRLC PDUを構成し、転送中に損失されたRLC PDUの再転送を担当する自動繰返し要求(ARQ:Automatic Repeat Request)機能を行うことができる。前記RLC階層23は上位階層から伝達されたRLC PDUを処理する方式に従い、透明モード(TM:Transparent Mode)、応答モード(AM:Acknowledged Mode)及び無応答モード(UM:Unacknowledged Mode)に区分され、前記RLC SDUまたはRLCPDUを格納するためのRLCバッファが存在する。

【0009】一方、前記RLC階層23とMAC階層24との間は論理チャンネル(LCH:Logical Channel)で接続され、現在、3GPPにはFDD(Frequency Division Duplex)用としてDTCH、DCCH、CTCH、CCCH、BCCH及びPCCHを含む6個の論理的チャンネルが使用されている。

【0010】専用トラフィックチャンネル(DTCH:Dedicated Traffic Channel)は特定使用者端末(UE)の専用データを伝達するためのチャンネルであり、専用制御チャンネル(DCCH:Dedicated Control Channel)は特定使用者端末(UE)の専用制御情報を伝達するためのチャンネルである。

【0011】共通トラフィックチャンネル(CTCH:Common Traffic Channel)は複数使用者端末(UE)の共通データを伝達するためのチャンネルであり、共通制御チャンネル(CCCH:Common Control Channel)は複数使用者端末(UE)の共通制御情報を伝達するためのチャンネルである。

【0012】また、ブロードキャスト制御チャンネル(BCCH:Broadcast Control Channel)はブロードキャスト情報を伝達するためのチャンネルであり、ページング制御チャンネル(PCCH:Paging Control Channel)はページング情報を伝達するためのチャンネルである。

【0013】そして、MAC階層24とPHY階層30との間は転送チャンネル(TCH:Transport Channel)で接続され、FDD用としてDCH、BCH、FACH、PCCH、RACH、CPCH及びDSCHを含む7

個の転送チャンネルを使用している。

【0014】専用チャンネル(DCH : Dedicated Channel)は特定使用者端末の専用データを伝達するためのチャンネルであり、ブロードキャストチャンネル(BC H : BroadcastChannel)はブロードキャスト情報を伝達するためのチャンネルである。

【0015】順方向接続チャンネル(FACH : Forward Access Channel)は順方向(下方)データを伝達するためのチャンネルであり、ページングチャンネル(PCH : PagingChannel)はページング情報を伝達するためのチャンネルである。

【0016】ランダム接続チャンネル(RACH : Random Access Channel)は逆方向(上方)データを伝達するためのチャンネルであり、共通パケットチャンネル(CP CH : CommonPacket Channel)は小さなパケットデータを伝達するためのチャンネルであり、ダウンリンク共有チャンネル(DSCH : Downlink Shared Channel)は順方向に多量のデータを伝達するためのチャンネルである。

【0017】多数の論理的チャンネル(L_CH)は一つの転送チャンネル(T_CH)に多重化(Multiplexing)でき、また、多数の転送チャンネル(T_CH)は一つの物理的チャンネルに多重化できる。

【0018】こうした無線インターフェースプロトコルにおいて、特定サービスを提供するために必要な階層及びチャンネルの特性を規定付ける無線ベアラーの設定(setup)過程が行われるが、このようなRBの設定過程は図2に示すとおりである。

【0019】図2は従来の無線インターフェースプロトコルにおける無線ベアラー設定方法を説明するための図である。図2を参照すれば、RBの設定はRRC階層204がピアRRC階層(peer RRC)201、上位階層(Higher layer)202及びBMC階層203の何れか一つまたは全部から各々無線ベアラー設定命令を受けた後(S211～S213)、データサービスに合う階層設定のために前記無線ベアラー設定命令を下位階層(BMC階層、PDCH階層、RLC階層、MAC階層、PHY階層)に伝達することにより設定される(S221～S225)。したがって、前記無線ベアラーの設定を通じてPDCH階層205の使用可否及びBMC階層203の使用可否が決定され、また、RLCモードにおいて、応答モード(AM : Acknowledged Mode)、無応答モード(UM : Unacknowledged Mode)、透明モード(TM : Transparent Mode)の何れか一つを使用するかが決定される。また、RLCエンティティ(entity)を生成しながらRLC階層とMAC階層との間にどの論理チャンネルを使用するか、MAC階層とPHY階層との間にどの転送チャンネルを使用するか、PHY階層でどの物理チャンネルを使用するかも決定される。このような具体的なパラメーター及び動作方法が設定されることにより一つ

の無線ベアラーが設定される。

【0020】ここで、RLC階層は他の階層とは異なり常に存在するものではなく、RBの設定時に生成され、該当サービスの提供後には消滅される特性を持っている。

【0021】現在、3GPPの規格では一つのRBは必ず一つのRLCエンティティを使用するように規定しており、RBは1使用者端末に最大32個まで同時に設定されるので、他の階層とは異なりRLCエンティティは同時に多数が存在できる。

【0022】前述するように、RLCエンティティは大きくRLCヘッダがつかない透明モード(TM : Transparent mode)と、RLCヘッダがつく非透明モード(Non-transparent mode)とに分れる。また、非透明モードは受信側からの応答信号(ACK)のある応答モードと、応答信号のない無応答モードとに分れる。

【0023】図3を参照して、RLC AMエンティティの構造を説明すれば、送信側(Transmitting Side)のAMエンティティは上位から降りてくるSDU(Service Data Unit)を大きさが一定なPDU(Protocol Data Unit)で作るために分割または連結(segmentation(concatenation))し(段階301)、ここにシーケンスナンバー(SN : Sequence Number)付きのヘッダを含む(段階302)。

【0024】ヘッダの含まれたPDUは、今後発生し得る再転送のために再送信バッファ(retransmission buffer)に格納される(段階303)。

【0025】一方、前記ヘッダの含まれたPDUは、マルチプレクサにより多重化した後(段階304)、データの保安のために暗号化する(段階305)。

【0026】次に、送信バッファ(transmission buffer)に一時格納されていてフィールドセッティングブロック(Setfields block)に伝達され(段階306)、フィールドセッティングブロックによりRLCヘッダのシーケンスナンバー(SN)を除外した他のフィールド(D/C及びPollfield等)が適正值でセッティングされて下位階層に伝達される(段階307)。

【0027】このように、上位から降りてきたデータ情報を載せたPDUをAMD(AM Data)PDUといい、その構造は図4に示す通りである。RLC階層は送信側への応答信号が不必要的場合に使用されるUMD(Unacknowledged Data)PDUと、応答信号が必要な場合に使用されるAMD(Acknowledged Data)PDUとの2種類形態のPDUが存在する。AMD PDUのフォーマットは図4に示すように、ヘッダ、L I部分(Length Indicator group)、データ、PAD(padding)またはピギーバックタイプの状態PDUからなる。

【0028】前記暗号化はAMD PDUだけに対して行なわれるが、この時、ヘッダ部分の初めの2オクテット(シーケンスナンバーを含んだ部分)は暗号化せず、その後の部分だけ暗号化する。

【0029】一方、受信段のAMエンティティは下位階層から伝達されたPDUを逆多重化させた後(段階308)、一旦受信バッファに格納させる(段階309)。そして、一つの完全なSDUを構成するPDUらが全部受信されれば、これらのPDUを復号化した後(段階310)、RLCヘッダを除去後(段階311)、SDU単位で再結合して上位階層に伝達する(段階312)。

【0030】一方、RLC UMエンティティは図5に示した。図5を参照すれば、送信側のUMエンティティは上位階層から降りてくるSDUを大きさが一定なPDUで作るために分割または連結し(段階511)、データ補完のためにPDUを暗号化させる(段階512)。以後、ここにシーケンスナンバーを含んだヘッダ付きのUMD PDUを構成し(段階513)、これらは転送バッファに格納されていって下位階層を通じて無線区間に転送される(段階514)。

【0031】前記UMD PDUの構造は図6に示す通りである。図6を参照すれば、前記UMD PDUのフォーマットはヘッダ、LI部分、データ、PADからなる。図6に示すように、前記UMD PDUのフォーマットで初めのオクテットはシーケンスナンバーの含まれたヘッダを示し、このヘッダ部分は暗号化せず、その以下の部分だけ暗号化する。

【0032】一方、受信側のUMエンタティティはUMD PDUを受信して一旦受信バッファに格納後(段階521)、一つの完全なSDUを構成するPDUらが前記受信側を通じて全部受信されれば、PDUらからRLCヘッダを除去させ(段階522)、続いて復号化過程をたどり(段階523)、SDU単位で再結合して上位階層に伝達する(段階524)。

【0033】このように、3GPPではユーザーデータの保護のために暗号化過程を行うが、前記暗号化過程はRLCモードによってAM及びUMの場合はRLC階層で、TMの場合はMAC階層で行われる。このとき、全てのデータに対して暗号化が行われるのではない。すなわち、AM及びUMの場合は論理チャンネル中のDTCHまたはDCCCHに転送されるデータだけに対して、TMの場合は転送チャンネル中のDCHに転送されるデータだけに対して暗号化が行われる。このような暗号化過程は各無線ベアラー別に設定されるものでなく、全ての無線ベアラーに対して一括して行われるか否かを決定することになる。

【0034】通常的に、暗号化したデータが送信側から受信側に転送されれば、受信側では復号化過程をたどりデータを復元することになる。このとき、送信側と受信側は同じアルゴリズムを使用し、同じ暗号化パラメータを使用しなければデータを正確に送受信できない。図3及び図5を参照すれば、より理解が容易になろう。

【0035】

【発明が解決しようとする課題】しかし、従来は全ての

無線ベアラーを対象として一括して暗号化可否を決定するため、無線ベアラー別に暗号化の行われない短所がある。すなわち、特定無線ベアラーに対しては暗号化を行い、他の無線ベアラーに対しては暗号化を行いたくない場合、従来の無線ベアラー設定方法としてはこれを支援できなかった。

【0036】例えば、現在BMCデータはRLC UMエンティティを使用し、論理的チャンネル中のCTCHを通じて転送され、このBMCデータはCTCHを使用するので暗号化が行われない。このようなBMCデータ中には暗号化が必要なデータもあり、暗号化が不必要的データもあるため、無線ベアラー別に選択して暗号化を行うべきである。すなわち、BMCサービスにはSMS-CB(Short MessageService - Cell Broadcast)、SMS-PP(Short MessageService-Point to Point)、IPマルチキャストなどのサービスがあるが、SMS-CBのような場合にはセル内の全てのユーザー端末(UE:UserEquipment)に知らせる情報を含んでいるので、暗号化を行わなくてもいい。

【0037】しかし、SMS-PPサービスは特定ユーザー端末が他の特定ユーザー端末だけに伝達するメッセージを含んでいるため、暗号化を行うべきであり、IPマルチキャストのような場合は特定グループのユーザー端末機だけに情報を伝達すべきであるため、やはり暗号化を行うべきである。ところが、従来の無線ベアラー設定方法によれば、SMS-PPサービス及びIPマルチキャストの場合、全ての端末に対して一括して暗号化可否が決定されることにより、暗号化サービスの差別化がなされないだけでなく、SMS-CBサービスとSMS-PPサービスを同時に使うことができない。

【0038】また、従来の無線ベアラー設定方法では、特定サービスを暗号化させて提供して、必要により暗号化を行いたくない場合、単純に該当無線ベアラーだけ暗号化を変更することができないので、全ての無線ベアラーを最初から再設定しなければならないという問題点があった。

【0039】また、全ての無線ベアラーの設定には、全ての階層に対する情報を全て再包含しなければならないので、多くの信号オーバーヘッド(Signalling overhead)を誘発させ、また、特定無線ベアラーの暗号化可否だけ変更適用するのに多くの時間遅延を発生させるという問題点も発生する。

【0040】よって、本発明は前記のような問題点を解決するためのもので、その目的は、無線ベアラー設定時にその暗号化の可否も共に設定して、各無線ベアラー別に暗号化を選択して行うための方法を提供することにある。

【0041】また、本発明の他の目的は、設定された無線ベアラーを利用してデータサービスを提供する途中またはデータの暗号化遂行中に暗号化遂行情報を変更す

るための方法を提供することにある。

【0042】

【課題を解決するための手段】前記目的を達成するために、本発明は、所定階層から無線資源制御(RRC)階層に暗号化遂行情報を伝達し、前記無線資源制御階層から前記暗号化遂行情報を無線リンク制御(RLC)階層に伝達し、前記無線リンク制御階層で前記暗号化遂行情報によってデータを暗号化させる段階を含んでなる無線ベアラー設定方法が提供される。

【0043】前記無線ベアラー設定方法によれば、前記所定階層は上位階層、ブロードキャスト/マルチキャスト制御(BMC)階層及びピア無線資源制御(peer RRC)階層を含むことができる。

【0044】前記無線ベアラー設定方法によれば、前記無線リンク制御(RLC)階層は無線ベアラーの設定時に生成されることがある。

【0045】前記無線ベアラー設定方法によれば、設定された無線ベアラーを利用してデータサービスの提供途中に前記暗号化遂行情報を変更できる。ここで、前記暗号化遂行情報の変更は前記所定階層から伝達される暗号識別子の変更によって行われる。

【0046】本発明の望ましい実施例によれば、無線ベアラー設定要求によって所定階層から無線資源制御(RRC)階層に暗号化遂行情報を伝達し、前記無線資源制御階層で前記無線ベアラー設定情報によって下位階層の無線ベアラーを設定し、前記無線ベアラー設定要求に応答して無線リンク制御(RLC)階層を生成し、前記無線リンク制御階層で前記暗号化遂行情報によってデータを暗号化させることを含んでなる暗号化遂行方法が提供される。

【0047】前記暗号化遂行方法によれば、前記無線ベアラー設定要求の発生時ごとに新しく生成される無線リンク制御階層により暗号化が行われる。

【0048】本発明の望ましい他の実施例によれば、無線リンク制御(RLC)階層で所定階層から伝達された暗号化遂行情報によってデータの暗号化を行い、前記所定階層で前記暗号化遂行情報を更新し、前記更新の暗号化遂行情報を前記無線リンク制御階層に伝達し、前記更新の暗号化遂行情報によって前記データの暗号化を行うことを含んでなる無線ベアラーの暗号化変更方法が提供される。

【0049】本発明の望ましいまた他の実施例によれば、無線資源制御(RRC)階層で所定階層からデータサービス要求とこれに対する暗号化遂行情報を伝達され、前記無線資源制御(RRC)階層がデータサービス要求に対応する無線リンク制御(RLC)階層と無線ベアラーを設定し、前記無線資源制御(RRC)階層で前記無線ベアラーに対する暗号化遂行情報を前記無線リンク制御階層に伝達し、前記無線リンク制御階層で前記暗号化遂行情報によって前記無線ベアラーを通じて伝達されるデータ

を暗号化することを含んでなるデータ暗号化方法が提供される。

【0050】前記データ暗号化方法によれば、前記無線資源制御階層が前記所定階層から無線ベアラー設定情報を伝達することができる。

【0051】また、本発明の無線ベアラー設定方法は、無線インターフェースプロトコルの無線ベアラーを設定する方法において、所定階層から無線資源制御(RRC)階層に暗号化遂行情報を伝達する段階と、前記無線資源制御階層で前記暗号化遂行情報を無線リンク制御(RLC)階層に伝達する段階と、前記無線リンク制御階層で前記暗号化遂行情報によってデータを暗号化させる段階を含んでなることを特徴とする。

【0052】さらに、前記所定階層から前記無線資源制御(RRC)階層に無線ベアラー設定情報を伝達する段階と、前記無線資源制御階層で前記無線ベアラー設定情報によって下位階層の無線ベアラーを設定する段階をさらに含む。

【0053】前記所定階層は上位階層、ブロードキャスト/マルチキャスト制御(BMC)階層及びピア無線資源制御(peer RRC)階層を含む。

【0054】前記暗号化遂行情報はNASメッセージを利用して前記上位階層から伝達される。

【0055】前記無線リンク制御(RLC)階層は無線ベアラー設定時に生成される。

【0056】さらに、設定された無線ベアラーを利用してデータサービスの提供途中に前記暗号化遂行情報を変更できる。

【0057】前記暗号化遂行情報の変更は前記所定階層から伝達される暗号識別子の変更によって行われる。

【0058】また、本発明は、無線インターフェースプロトコルの暗号化を行う方法において、無線ベアラー設定要求によって所定階層から無線資源制御(RRC)階層に暗号化遂行情報を伝達する段階と、前記無線資源制御階層で前記無線ベアラー設定情報によって下位階層の無線ベアラーを設定する段階と、前記無線ベアラー設定要求に応答して無線リンク制御(RLC)階層を生成する段階と、前記無線リンク制御階層で前記暗号化遂行情報によってデータを暗号化させる段階とを含んでなることを特徴とする。

【0059】前記無線ベアラー設定要求の発生時ごとに新しく生成される無線リンク制御階層により暗号化が行われる。

【0060】前記所定階層は上位階層、ブロードキャスト/マルチキャスト制御(BMC)階層及びピア無線資源制御(peer RRC)階層を含む。

【0061】前記暗号化遂行情報は暗号識別子である。

【0062】また、本発明は、無線ベアラーの暗号化を変更する方法において、無線リンク制御(RLC)階層で所定階層から伝達された暗号化遂行情報によってデータ

の暗号化を行う段階と、前記所定階層で前記暗号化遂行情報を更新する段階と、前記更新の暗号化遂行情報を前記無線リンク制御階層に伝達する段階と、前記更新の暗号化遂行情報によって前記データの暗号化を行う段階とを含んでなることを特徴とする。

【0063】前記所定階層は上位階層、ブロードキャスト/マルチキャスト制御(BMC)階層及びピア無線資源制御(peer RRC)階層を含む。

【0064】前記暗号化遂行情報は暗号化の可否を示す。

【0065】前記暗号化遂行情報は暗号識別子である。

【0066】本発明のデータ暗号化方法は、移動通信送受信装置において、無線資源制御(RRC)階層がデータサービス要求に対応する無線リンク制御(RLC)階層と無線ベアラーを設定する段階と、前記無線資源制御階層で前記無線ベアラーに対する暗号化遂行情報を前記無線リンク制御階層に伝達する段階と、前記無線リンク制御階層で前記暗号化遂行情報によって前記無線ベアラーを通じて伝達されるデータを暗号化する段階とを含んでなることを特徴とする。

【0067】前記無線資源制御階層が所定階層からデータサービス要求とこれに対する暗号化遂行情報を伝達される段階をさらに含む。

【0068】前記無線資源制御階層が前記所定階層から無線ベアラー設定情報を伝達される。

【0069】前記所定階層は上位階層、ブロードキャスト/マルチキャスト制御階層、ピア無線資源制御階層の何れか一つであることを特徴とする。

【0070】前記設定された無線ベアラーを利用してデータサービスの提供途中に前記暗号化遂行情報が変更できる。

【0071】前記暗号化遂行情報の変更は前記所定階層から伝達される暗号識別子の変更によって行われる。

【0072】

【発明の実施の形態】以下、添付図面に基づき、本発明の実施例を詳細に説明する。

【0073】図7は本発明に係る無線インターフェースプロトコルにおける無線ベアラー設定方法を説明するための図である。本発明に係る無線ベアラー設定方法は、上位階層、ピアRRC階層、BMC階層中の少なくとも一つが無線資源制御(RRC)階層に無線ベアラー設定を要請する時、暗号化遂行可否も共に伝達し、前記RRC階層は前記要請によって下位階層に無線ベアラーを設定すると同時にRLC階層に暗号化遂行可否を伝達して、データの暗号化可否を決定する。このとき、上述したように、前記無線リンク制御(RLC)階層は無線ベアラーの設定時ごとに生成し得るのに注意すべきである。

【0074】図7を参照してこれを説明すれば、特定端末(UE)に互いに異なるサービス提供のためにピアRRC階層701、上位階層702、BMC階層703から

RRC階層704に無線ベアラー設定命令が各々伝達される時、暗号化遂行情報をも共に伝達される(S611～S613)。ここで、前記暗号化遂行情報を暗号化の可否を示すもので、暗号識別子(CipheringIndicator)であるのが望ましい。これを階層別により具体的に説明すれば次の通りである。

【0075】1) 上位階層から無線ベアラー設定命令及び暗号化遂行情報をRRC階層に伝達される場合(S612)、上位階層702から下位階層にあるサービスを

10 提供する場合、まず、下位階層の無線ベアラーを設定するために前記上位階層702は自身の下位階層のRRC階層704に無線ベアラー設定命令を行う(S612)。

これをNAS(Non Access Stratum; ASの上位部分)メッセージというが、前記NASメッセージは制御プレーン(Controlplane)に位置し、NASからAS(Access Stratum; RRC階層、BMC階層、PDCP階層、RLC階層、MAC階層、PHY階層などを含む部分)にRRC SAP(Service Access Point)を通じて伝達される(図8)。ここで、RRC SAPにはGC(General Control) SAP、Nt(Notification) SAP、DC(DedicatedControl) SAPの3種類が存在する。したがって、前記NASメッセージを利用して無線ベアラー設定命令が前記RRC階層704に伝達される時、暗号識別子もNASメッセージに含まれて伝達される。前記NASメッセージを伝達されるRRC階層704は自身の下位階層すなわちBMC階層703、PDCP階層705、RLC階層706、MAC階層707、PHY階層708等にサービスに合うように無線ベアラーを設定することになる(S621～S625)。

また、前記RRC階層704は前記RLC階層706に暗号識別子を伝達する。すると、前記RLC階層706は前記暗号識別子によってデータの暗号化を行う。このとき、BMC階層及びPDCP階層はサービスによって使用することもあり、使用しないこともある。

【0076】2) ピアRRC階層から無線ベアラー設定命令及び暗号化遂行情報をRRC階層に伝達される場合(S611)、ピアRRC階層のRB設定過程は前記上位階層による無線ベアラー設定過程の一部であって、前記上位階層702であるサービスを提供する場合、自身の下位階層を設定すると同時に自身のピアエンティティも

40 設定する。前記のような過程を通じて転送したいデータがピアRRC階層701まで伝達される。このために、上位階層702から無線ベアラー設定命令を受けたRRC階層704Fは、自身のピアRRC階層701に情報要素(Information Element)を通じて前記無線ベアラー設定命令を知らせる。これを伝達されたピアRRC階層701はやはり自身の下位階層を設定することになる(S611)。一方、前記情報要素に暗号化可否を知らせるための暗号識別子を挿入することにより、前記RLC階層706によるデータの暗号化が行われる。ここで、

前記上位階層702とピアRRC階層701を区分することは、一つのRRC階層704の立場から見れば、無線ベアラー設定命令がNASで伝達されることもあり、ピアRRC階層で伝達されることもあるためである。

【0077】3) BMC階層から無線ベアラー設定命令及び暗号化遂行情報がRRC階層に伝達される場合(S613)、ブロードキャスト/マルチキャストサービスの機能はCBC(Cell BroadcastCenter)であるが、これはコアネットワーク(CN:Core Network)に位置している。あるブロードキャスト情報を転送したい場合、CBCはBMC階層703に無線ベアラー設定命令を行い、前記BMC階層703は自身のRRC階層704にプリミティブ(primitive)を通じて前記無線ベアラー設定命令を伝達する(S613)。このとき、暗号識別子が前記プリミティブに挿入され伝達され、前記プリミティブを伝達されるRRC階層704は自身の下位階層を設定し、同時に相手方RRC階層に知らせて相手方の下位階層が設定されることができる。また、前記BMC階層703は暗号識別子をRLC階層706に伝達してデータを暗号化させることができる(S621~S625)。

【0078】一方、前記上位階層702、ピアRRC階層701、BMC階層703から伝達される情報はユーザーデータではない制御情報を知らせる信号メッセージなので、PDUやSDUのような特定形態なしに次の通り名前のみ定義される。すなわち、上位階層702の場合はNASメッセージ、RRC階層701の場合は情報要素、BMC階層703の場合はプリミティブを通じて無線ベアラー設定命令及び暗号識別子が各々伝達される。

【0079】前記で説明したように、RRC階層704が無線ベアラー設定命令と暗号化遂行可否を要請される場合、前記RRC階層704はプリミティブを通じて下位階層に命令を行うことになる。

【0080】一般的に、暗号化はRLC階層とMAC階層で行うが、MCA階層の場合は全ての無線ベアラーが共通的に使用するので、無線ベアラー別に暗号化する必要がない。ところが、RLC階層の場合は無線ベアラー別に生成されるので、選択して暗号化することができる。

【0081】前記RLC階層の場合、無線ベアラー別の暗号化はAM及びUMだけで行われ、TMの場合はMAC階層で暗号化を行うので、無線ベアラー別の暗号化を行わなくてもよい。

【0082】そして、RLC AMまたはUMがRRC階層から無線ベアラー設定命令を伝達されれば、他のパラメーターを設定する同時に暗号化可否を判断し、その判断の結果、暗号化を行うべき場合はデータを暗号化してMAC階層707に伝達し、暗号化を行わないべき場合は暗号化しなくて直ぐMAC階層707にデータを伝達する。

【0083】したがって、前記RRC階層704がBMC階層703を設定する場合、前記RRC階層704はBMC階層703にCBMC-COMFIG-REQを利用してCTCH環境(configuration)設定情報を伝達する(S621)。

【0084】また、前記RRC階層704がPDCP階層705を設定する場合、前記RRC階層704がPDCP階層705にCPDCC-COMFIG-REQを利用してヘッダ圧縮(header compression)情報、RLC-SAP情報(AM/UM/TM中のどのRLCを使用するか)、PDCPシーケンスナンバーの同期化遂行可否を伝達する(S622)。

【0085】また、前記RRC階層704がRLC階層706を設定する場合、前記RRC階層704がRLC階層706にCRLC-COMFIG-REQを利用してRLCAM、UMまたはTM中の必要なモード選択及びRLCエンティティ生成、暗号化要素(CipheringElement-Cipheringモード、暗号化に必要なCiphering Key値及びRLC_HFN(Hyper Frame Number)値、暗号化を始めるPDUのSN-AM及びUMだけ該当)、各モードに必要なパラメーターを伝達する(S623)。ここで、パラメーターは、AMの場合はPDUsize、In-sequence Delivery indication、Timer value、Protocol parameter value、Pollingtrigger、Status trigger、SDU discard modeなどを含み、UMの場合はTimer valueを含み、TMの場合はTimervalue、Segmentation indicationを含む。

【0086】前記RRC階層704はCMAC-COMFIG-REQを利用してユーザー端末情報(UEinformation-S-RNTI、C-RNTI、SRNC identity, Activation time)、RBinformation(Transport channel identity、Logical channel identity、MAClogicalchannel priority)、Transport channel information(Transport Format CombinationSet)、Ciphering Element (RLCがTMの時だけ使用-Ciphering mode、Ciphering Key値及びMAC_HFN値)を伝達してMAC階層707を設定できる(S624)。

【0087】前記RRC階層704はCPHY-TriCH-COMFIG-REQまたはCPHY-RL-Setup-REQなどをPHY階層708に伝達する(S625)。

【0088】上述したように、RRC階層704は各階層にプリミティブを利用して無線ベアラー設定命令を伝達して無線ベアラーに合う環境を設定できる。

【0089】一方、前記プリミティブ等は無線ベアラー設定途中にいつでも再設定される。すなわち、あるパラメーターを変更したい場合、これを含むプリミティブをRRC階層に再送することにより、該当パラメーターのみを変更できる。

【0090】無線ベアラー別の選択的な暗号化を適用す

る場合、RRC階層からRLC階層へのCRLC-CO-NF1G-REQプリミティブに暗号識別子というパラメーターが追加される。

【0091】また、RLC AMエンティティまたはUMエンティティで暗号化遂行可否が可変的に調整できる。すなわち、CRLC-CONF1G-REQプリミティブを通じて該当RLCエンティティが暗号化するか否かを知らせるが、このような暗号化遂行可否は暗号化遂行途中にデータを暗号化したくない場合、さらにCRLC-CONF1G-REQプリミティブを通じて暗号化遂行可否の変更が行われる。

【0092】また、無線ペアラーは使用中に各設定に対して前記で説明した3つのシグナルリングを通じていつでも暗号化遂行情報が変更でき、RRC階層は前記暗号化遂行情報によってRLC階層のデータを暗号化させることができる。例えば、はじめにデータを暗号化させる暗号化遂行情報によってデータが暗号化した場合、変更されてデータを暗号化させない暗号化遂行情報によってデータが暗号化されない。

【0093】一方、ピアRRC階層701、上位階層702、BMC階層703の各階層の提供するサービスが互いに異なるため、RRC階層がピアRRC階層、上位階層、BMC階層中の一つまたは一つ以上から無線ペアラー設定命令を伝達されることも出来る。このような場合にも前記暗号化遂行可否が上述したシグナルリングを通じて伝達されることで、常に暗号化遂行可否がRRC階層に伝達され、RRC階層は下位階層設定及び暗号化遂行情報を下位階層に知らせる。

【0094】

【発明の効果】したがって、本発明に係る無線ペアラーの設定方法によれば、無線ペアラー別に選択的な暗号化を行うことで、3GPPにおいて多種多様なサービスを

同時に支援できる。

【0095】また、本発明に係る無線ペアラーの設定方法によれば、設定された無線ペアラーを利用してデータサービスの提供途中に暗号化遂行情報を変更でき、時間遅延を防止してより迅速なサービスを提供できる。

【図面の簡単な説明】

【図1】3GPPの無線インターフェースプロトコルの構造を示す構成図である。

【図2】従来の無線インターフェースプロトコルにおける無線ペアラー設定方法を説明するための図である。

【図3】RLC AMエンティティの構造を示す図である。

【図4】図3でRLC AMD PDUのフォーマット構造を示す図である。

【図5】RLC UMエンティティの構造を示す図である。

【図6】図5でRLC UMD PDUのフォーマット構造を示す図である。

【図7】本発明に係る無線インターフェースプロトコルにおける無線ペアラー設定方法を説明するための図である。

【図8】本発明に係るRRC SAPを説明するための図である。

【符号の説明】

10 10、204、704 RRC階層

21 205、705 PDCP階層

22 203、703 BMC階層

23 706 RLC階層

24 707 MAC階層

30 30、708 PHY階層

201 701 ピアRRC階層

202 上位階層

203 BMC

204 RLC

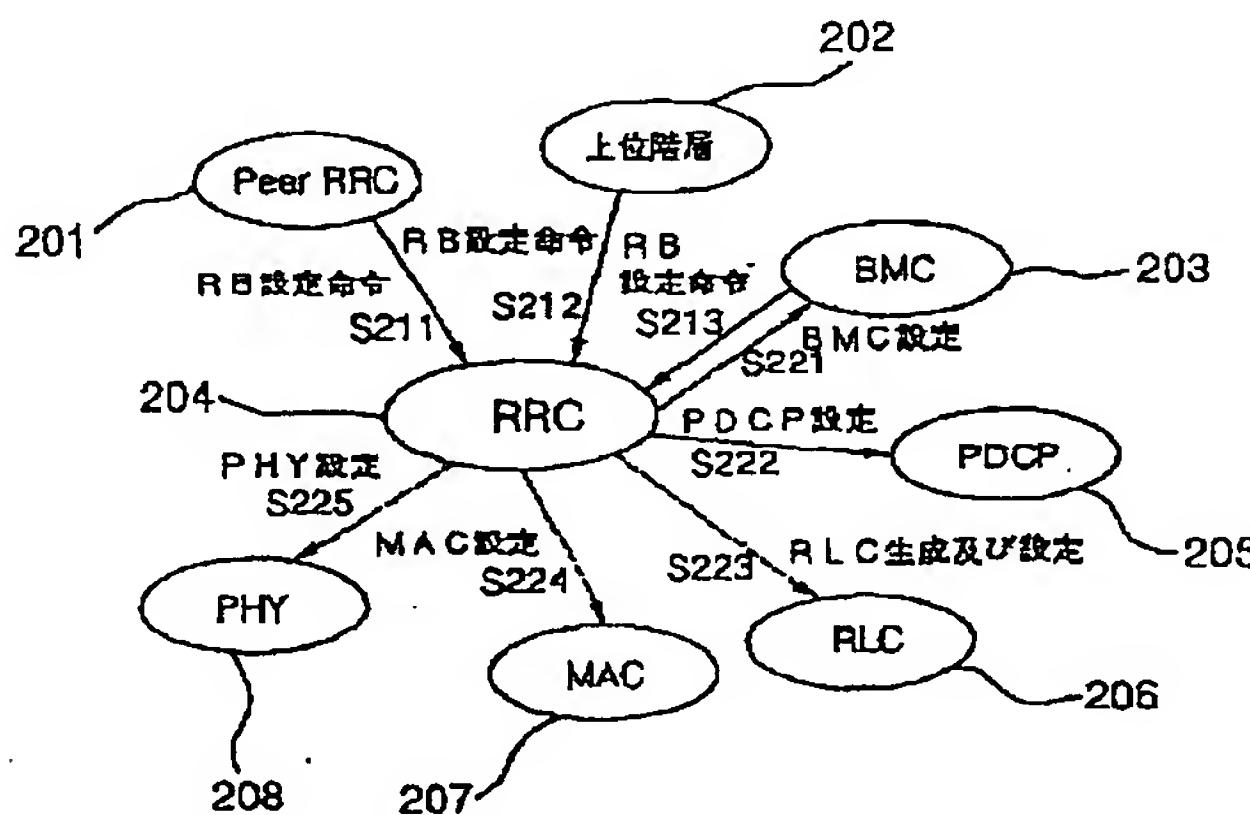
205 PDCP

206 MAC

207 PHY

208 RRC

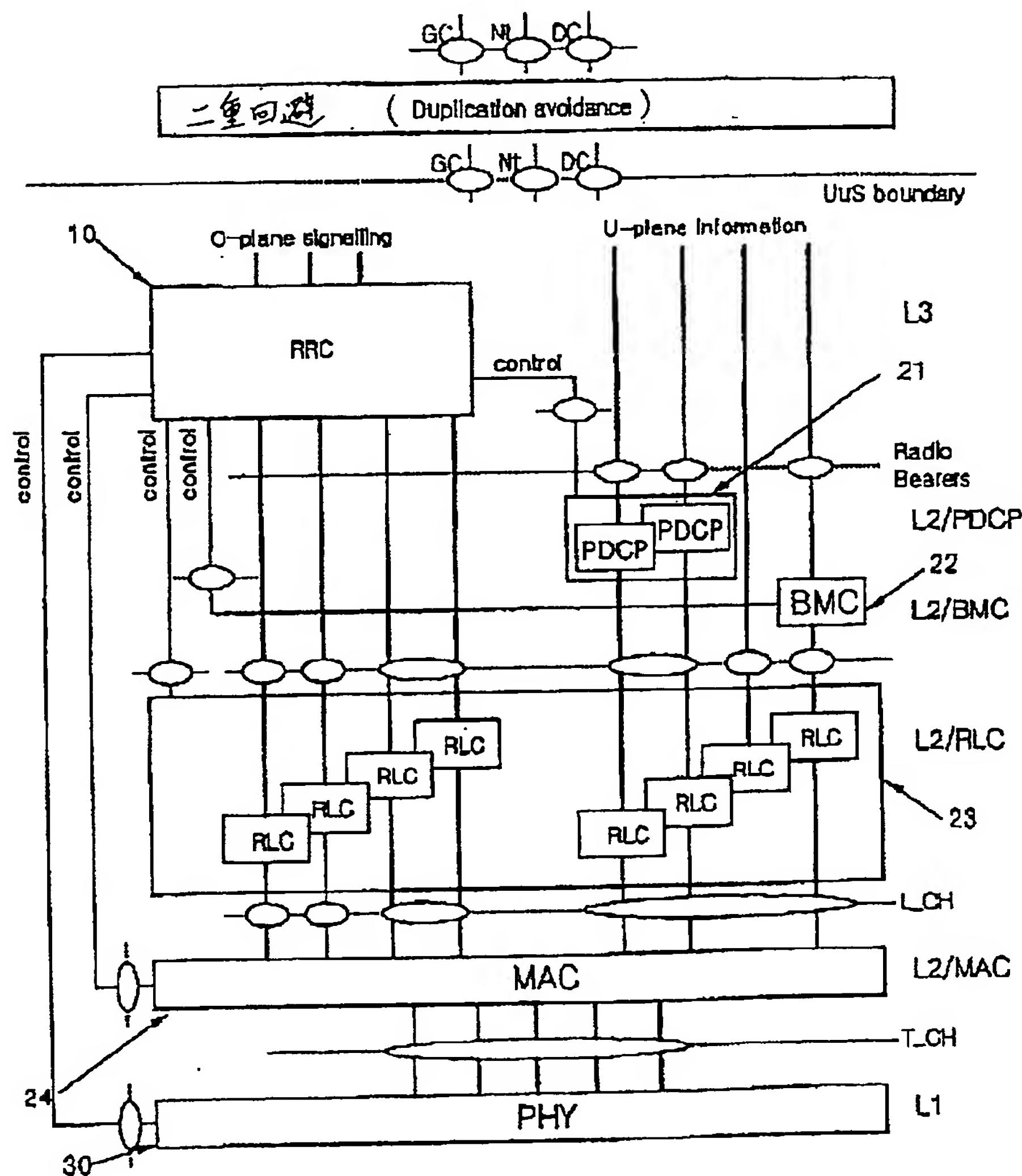
【図2】



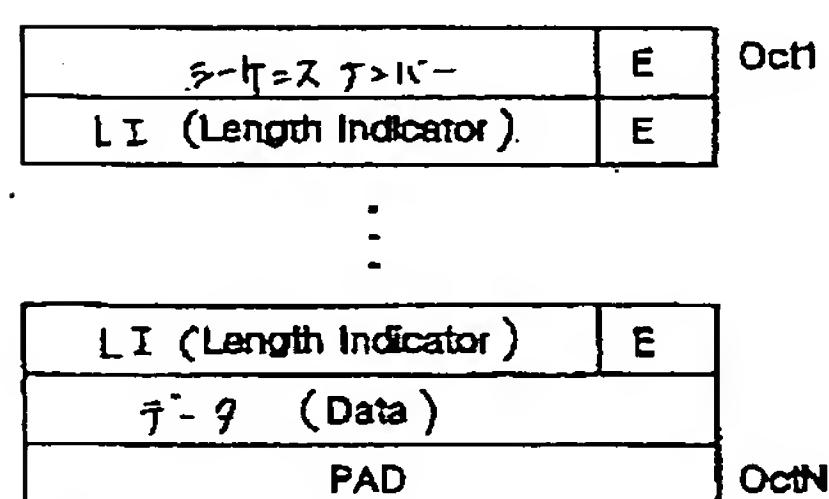
【図4】

D/C	シーケンスナンバー	Oct1
シーケンスナンバー	P	Oct2
レI (Length Indicator)	E	Oct3
:		
レI (Length Indicator)	E	OctN
データ (Data)		
PADまたはビギ バックタイプの基PDU		

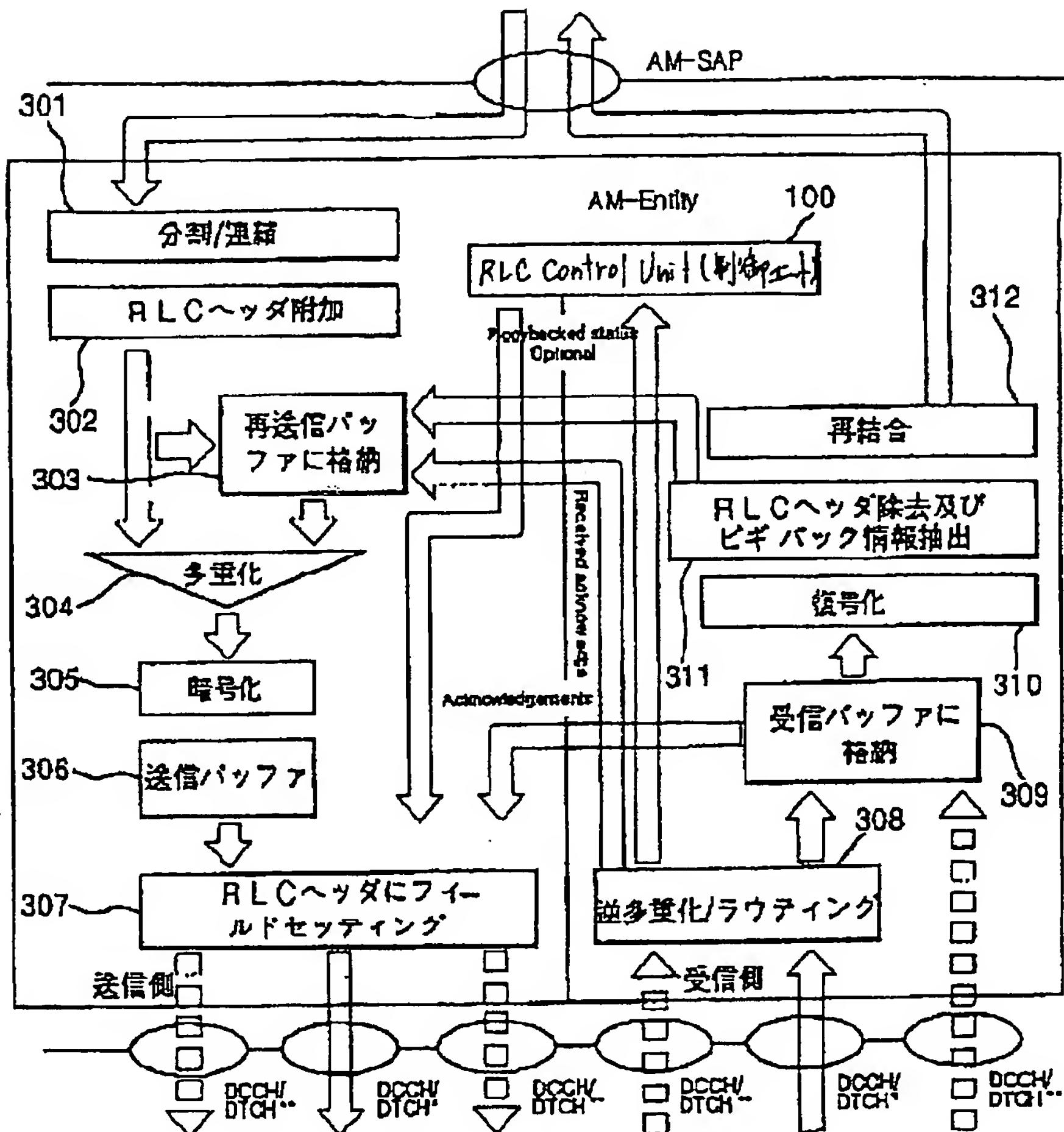
【図1】



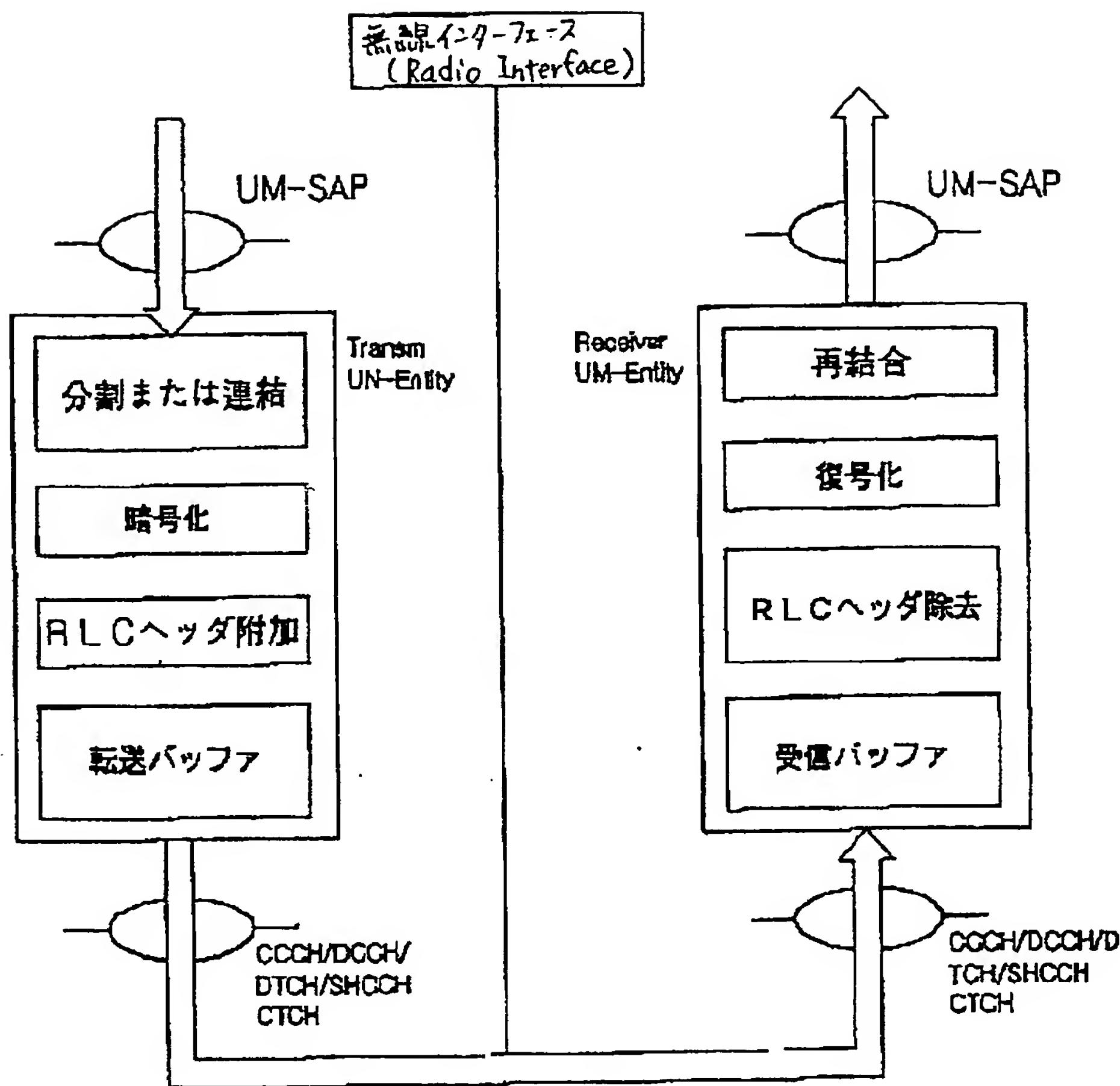
【図6】



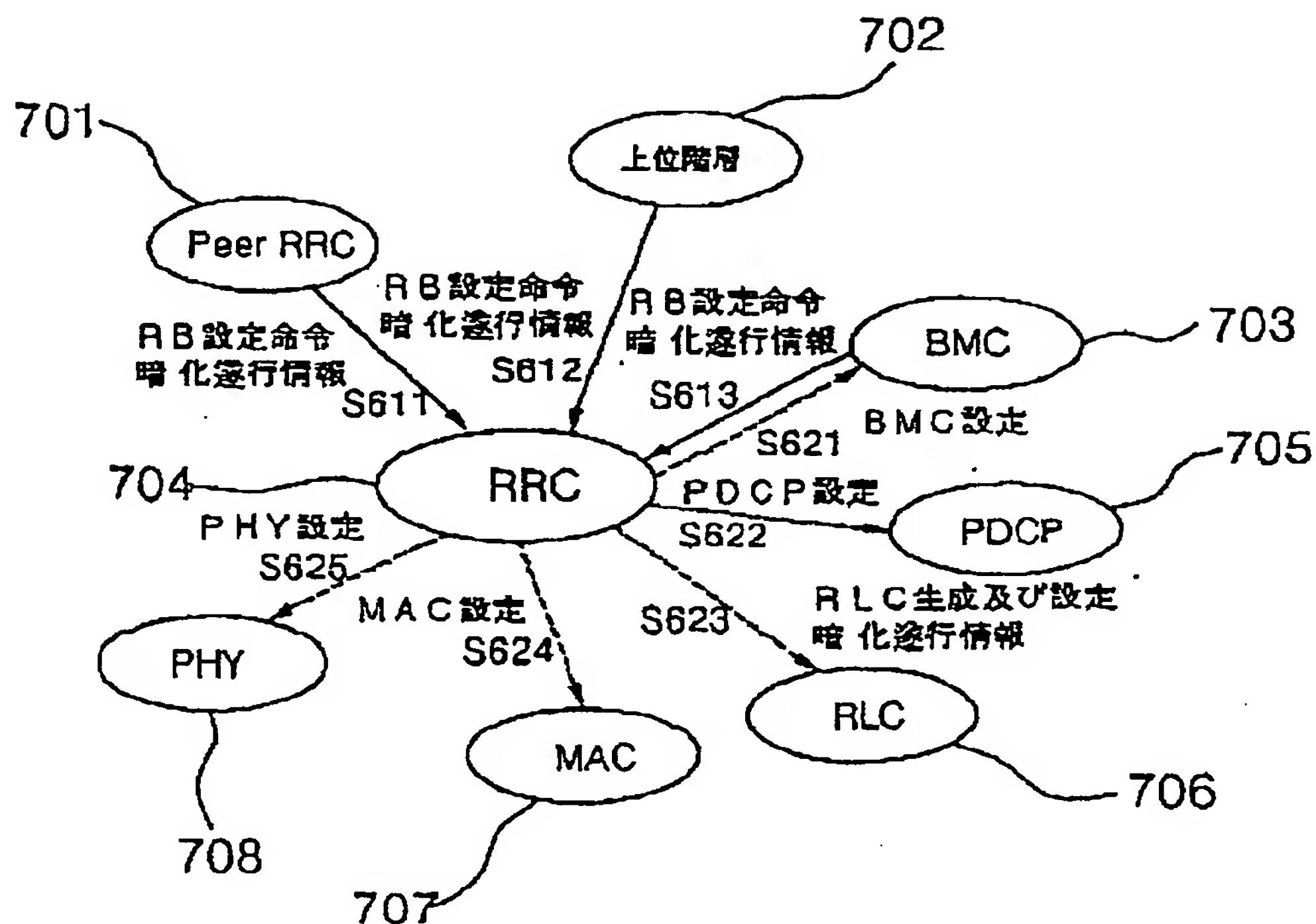
【図3】



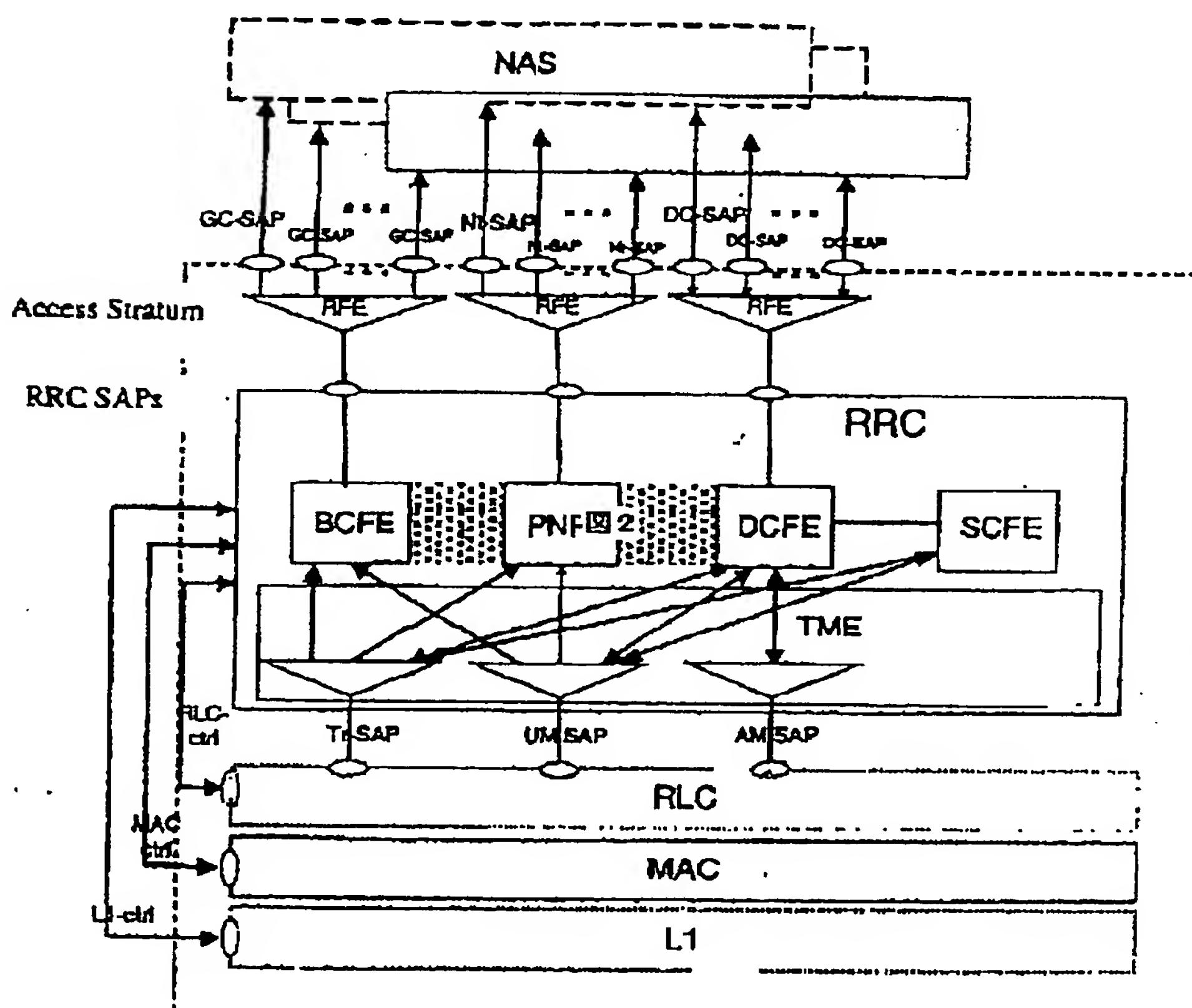
【図5】



【図7】



【図8】



フロントページの続き

F ターム(参考) 5J104 AA01 AA32 CA02 EA16 NA02

PA01

5K033 AA02 AA03 AA08 CB14 DA17

EC01